Office of Cyber-Security
& Information Assurance

Oik son Shickyrys Lectraneagh as Sauchys Fysseree

CSC

Cyber Security Centre
for the Isle of Man

NATIONAL INFRASTRUCTURE SECURITY BILL (NISB)

Consultation Response

1. Background

Isle of Man residents should have confidence in the security and resilience of national infrastructure sectors to deliver essential goods and services. Essential services – such as our electricity grid, water supply and telecommunications systems should be able to withstand and recover from hazards that might disrupt their functions.

Unfortunately, hostile entities and criminals have recognised that this dependency creates an opportunity for what have become known as ‘cyber-attacks’.

The Department of Home Affairs wishes to introduce a National Infrastructure Security Bill to raise levels of security and resilience for core services on the Isle of Man, which rely heavily on digital services.

The Department ran a consultation to seek views from interested parties on the draft National Infrastructure Security Bill.

This report provides a summary of the responses received.

2. Overview of responses

The public consultation opened on the 1st of December 2025 and closed on the 9th of January 2026. The Department received **13** responses to the consultation, 8 of which were received via the consultation hub. The **13** responses comprised:

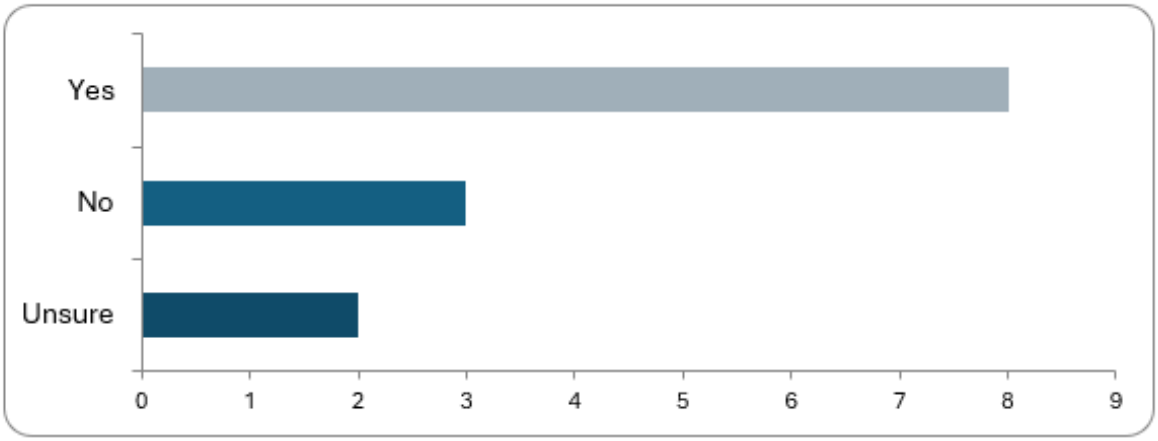
- **5** Members of the public
- **4** Private Companies
- **1** Government Departments, Offices or Boards
- **3** Local Authorities

The comments in the summary of responses reflect where respondents said their response could be published.

Section 1: Fundamental Principles

Q1: Do you find the definitions of "national infrastructure" and "critical national infrastructure" in Clause 3(1) clear and sufficient for identifying relevant sectors and assets?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	*8*	61.54%
No	*3*	23.08%
Unsure	*2*	15.38%
Not Answered	*0*	0.00%

Commentary

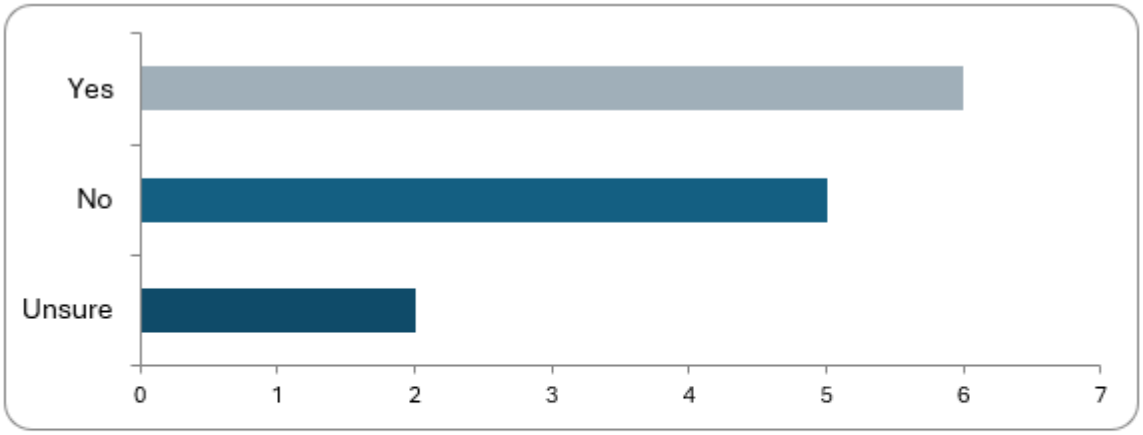
Based on the responses received, most respondents agreed that the definitions of national infrastructure and critical national infrastructure were felt to be clear and sufficient.

Where respondents were unsure or answered that the definition was not clear, this reflected uncertainty as to whether the sector they represented would fall under the definition of national and critical national infrastructure.

This was also reflected in the responses to question 5 and our response to these concerns is addressed in question 5.

Q2: Is the definition of a "security incident" in Clause 4 comprehensive and appropriate?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	*6*	46.15%
No	*5*	38.46%
Unsure	*2*	15.38%
Not Answered	*0*	0.00%

Commentary

Responses did support the definition of a security incident in clause 4.

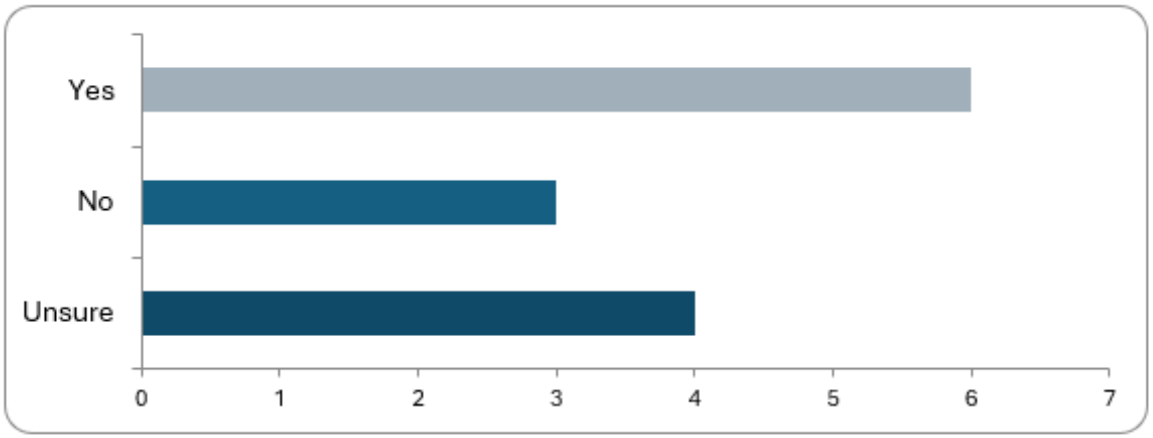
For those respondents who disagreed and provided comments it was apparent there was a misinterpretation of the question and/or a misunderstanding of the background and mechanisms adopted.

The definition of a security incident should also be read in conjunction with Clauses 30 and 31 regarding the obligations to report and the understanding that the Critical National Infrastructure comprises a wide variety of services providers some of whom are highly specialised.

Section 2: Provider Classification and Registration

Q3: Are the three classifications of essential, important and unclassified enough to make regulations in respect of an assurance framework?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	6	46.15%
No	3	23.08%
Unsure	4	30.77%
Not Answered	0	0.00%

Commentary

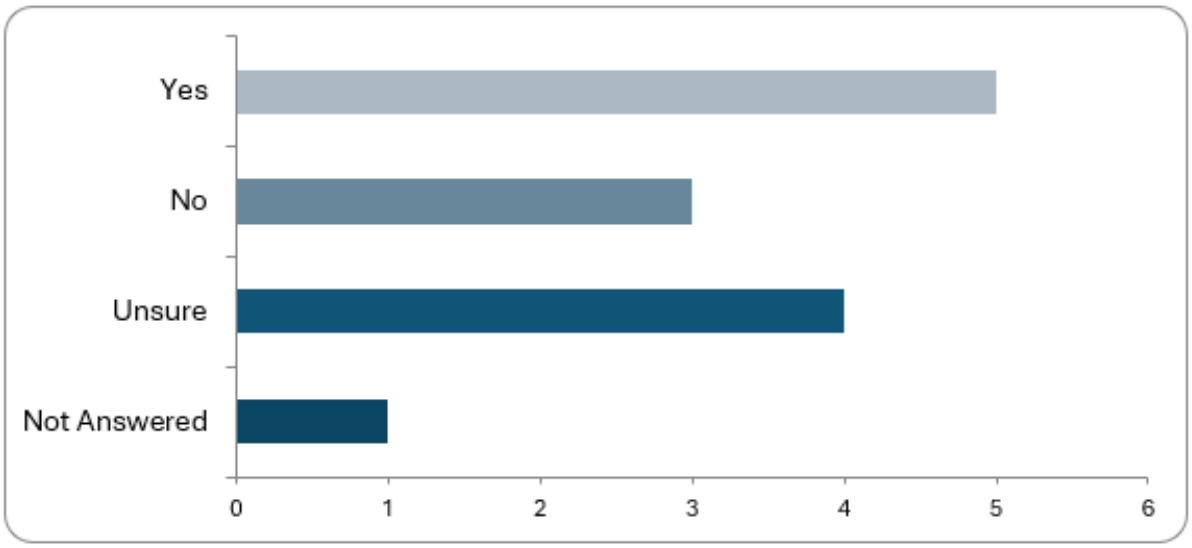
In the main the respondents supported the 3 classifications.

Where the responses were not supportive of the classifications concerns were related to the definition of national and critical national infrastructure which were also raised in questions 1 and 5. This is addressed in the commentary for question 5.

One respondent commented:
"The three-tier model is logical and allows proportional regulation..."

Q4: Do the registration requirements in Clause 10 and the ongoing conditions in Clause 11 provide sufficient clarity and flexibility.

*There were **13** responses to this question.*



Option	Total	Percent
Yes	*5*	38.46%
No	*3*	23.08%
Unsure	*4*	30.77%
Not Answered	*1*	7.69%

Commentary

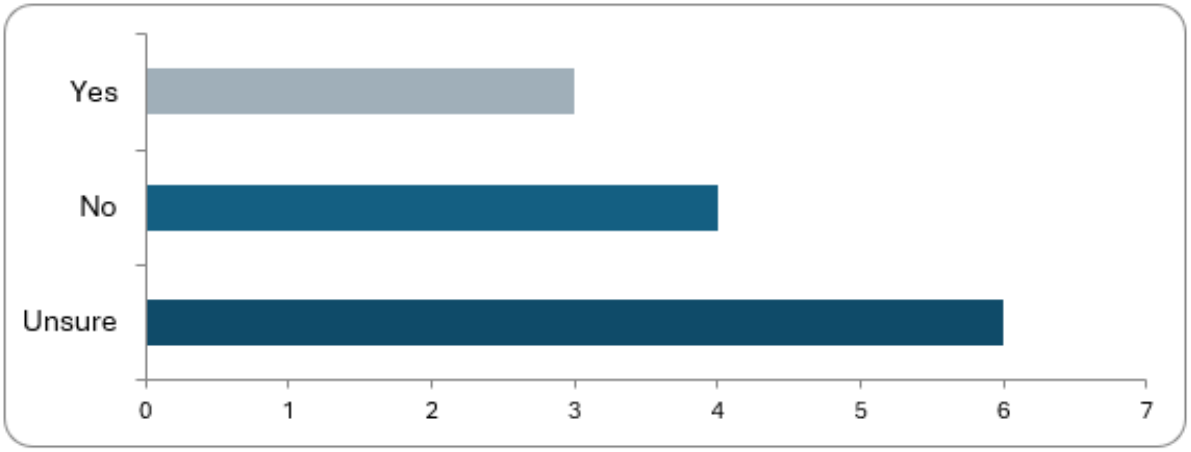
Whilst the majority were in favour the comments provided suggested more detail was needed.

The detail behind clauses 10 and 11 will be provided through secondary legislation in the form of regulations and Codes of Practice as appropriate. Such matters will be subject to separate consultation as they are developed.

One comment was as follows:
"These requirements match other well established regulatory registration requirements."

Q5: Are providers appropriately allocated in schedule?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	3	23.08%
No	4	30.77%
Unsure	6	46.15%
Not Answered	0	0.00%

Commentary

Commentary, particularly from those respondents who answered NO, identified enhancements to the definitions which could clear up any ambiguity.

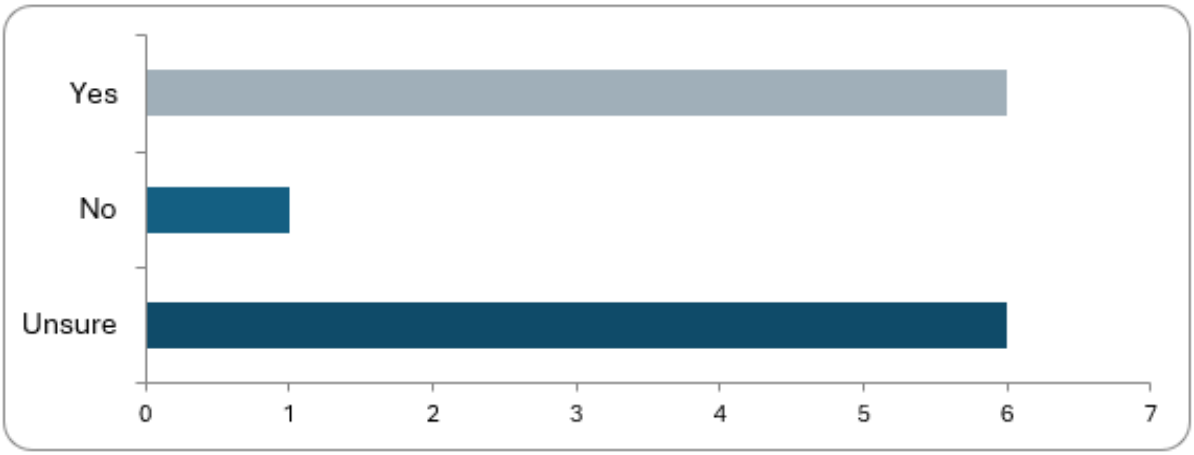
The Department will look to amend the definitions highlighted to address these concerns.

Research across other jurisdictions identified potentially highly bureaucratic methods involving gross profit and other indicators. Whilst all these had been considered they were discounted in favour of implementing a compliance framework rather than an investigatory or oversight regime which could be both resource and cost intensive. The result was to use the criticality of the service and the number of workers engaged in that service.

Section 3: Resilience and Cybersecurity Standards

Q6: Is the division of responsibilities between the Department (Clause 12) and responsible authorities (Clause 7 & 9) for setting resilience and cybersecurity standards clear and workable?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	6	46.15%
No	1	7.69%
Unsure	6	46.15%
Not Answered	0	0.00%

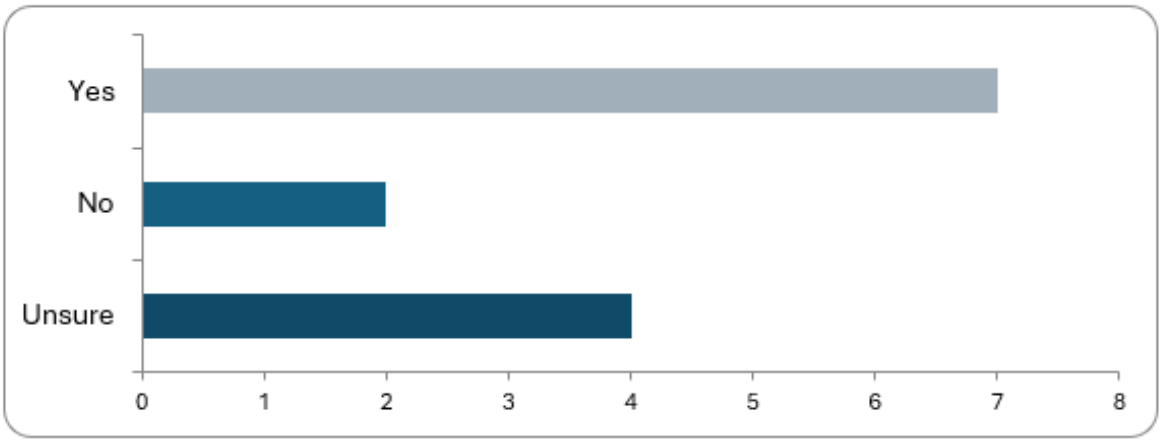
Commentary

Responses were split equally between those who agreed with the division of responsibilities and those who were unsure. This reflected uncertainty from some respondents who were not clear if they would be in scope of the proposed legislation, and as a result if they would need to interact with either the responsible or technical authority. One respondent commented:
"The division of responsibilities is appropriate; however we note there is scope for the Department to set mandatory standards, we would ask, that with this in mind, the Department commits to only setting standards that align with other well-established standards and governance frameworks. Such standards and frameworks include COBIT NIST, ISO27001 and ISO27002 and SOC2."

This is the intended approach to setting standards.

Q7: Are the consultation and publication requirements in Clause 12(2)–(3) sufficient to ensure transparency and stakeholder engagement?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	7	53.85%
No	2	15.38%
Unsure	4	30.77%
Not Answered	0	0.00%

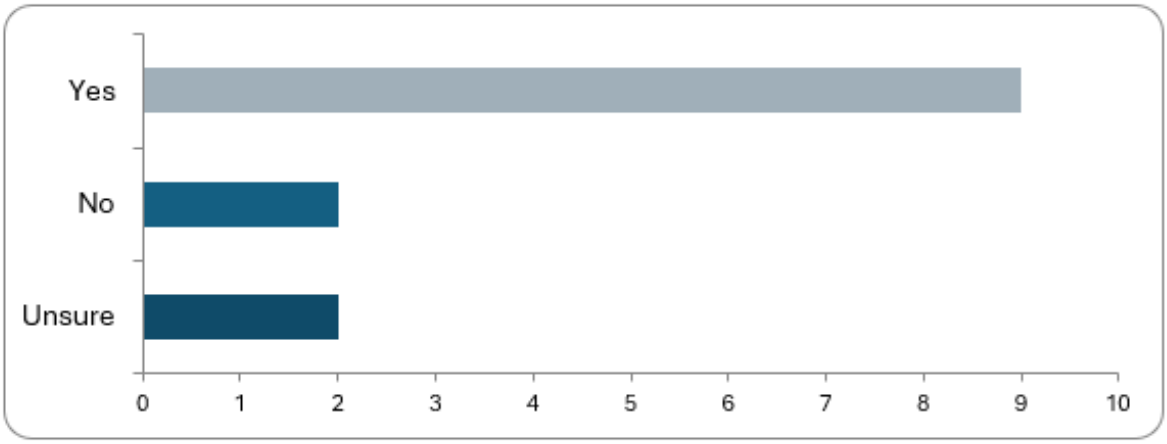
Commentary

Responses supported the proposed consultation and publication requirements in clause 12(2)-(3).

Section 4: Responsibilities of the Technical Authority

Q8: Are the responsibilities of the Technical Authority clearly defined and appropriate?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	9	69.23%
No	2	15.38%
Unsure	2	15.38%
Not Answered	0	0.00%

Commentary

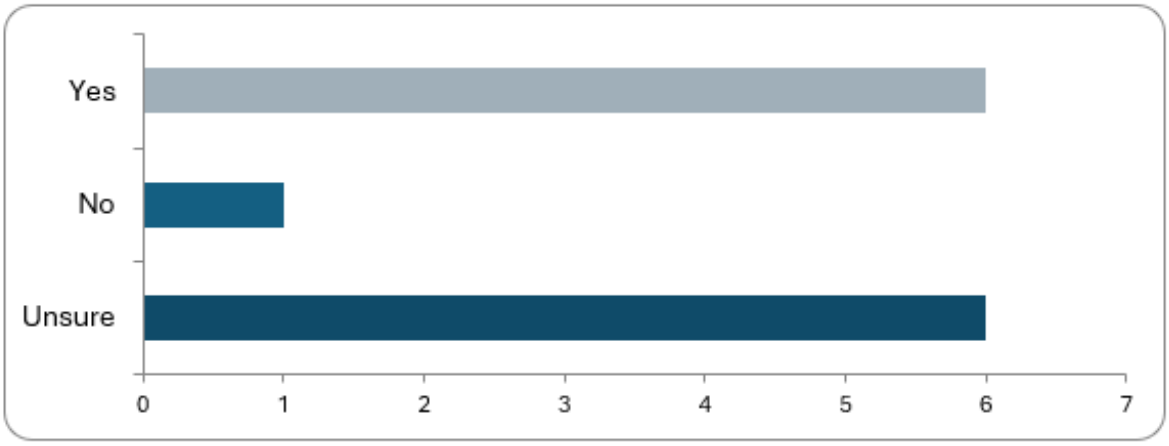
Most responses agreed that the responsibilities of the Technical Authority were clearly defined and appropriate.

Some comments were as follows:
"We feel this is well defined and appropriate."

"The Technical Authority's remit is clearly framed around technical cyber-security functions and coordination, which is appropriate and proportionate."

Q9: Does the role of the Technical Authority provide sufficient support to registered providers?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	6	46.15%
No	1	7.69%
Unsure	6	46.15%
Not Answered	0	0.00%

Commentary

Most responses agreed that the role of the Technical Authority would provide sufficient support to registered providers.

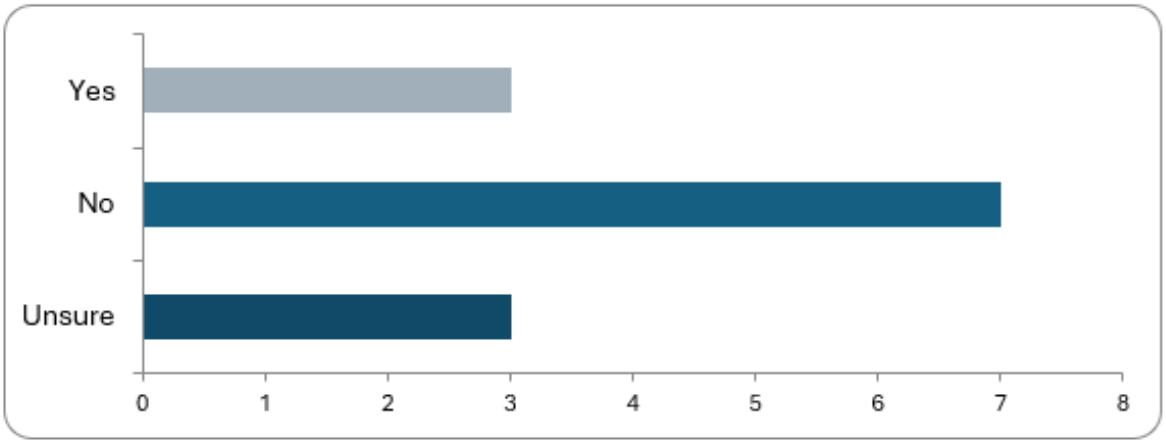
For those who responded as unsure, comments asked more detailed questions as to how the Technical Authority would operate in practice, which can be addressed through stakeholder engagement.

Some comments were as follows:
"The advisory and coordinating functions appear well designed, particularly for incident response and guidance."

"As written, yes, processes, procedures and SLAs would be required to ensure this support is delivered as intended."

Q10: Are there additional functions the Technical Authority should undertake?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	3	23.08%
No	7	53.85%
Unsure	3	23.08%
Not Answered	0	0.00%

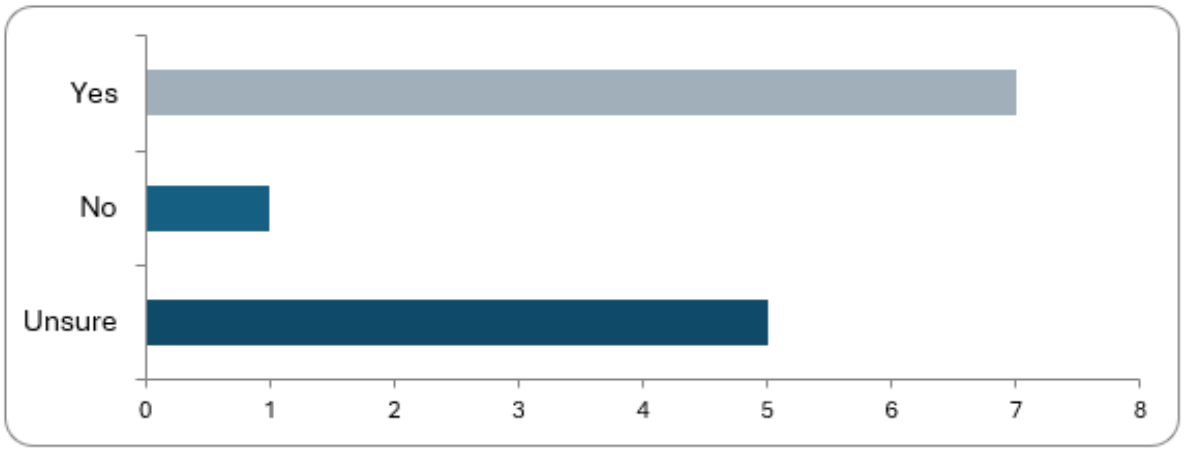
Commentary

Respondents generally did not think there was a need for any additional functions.

Section 5: Incident Notification and Reporting

Q11: Are the timeframes for incident notification and reporting in Clauses 31–32 (24-hour notification, 72-hour interim, one-month final) appropriate and achievable?

*There were **13** responses to this question.*



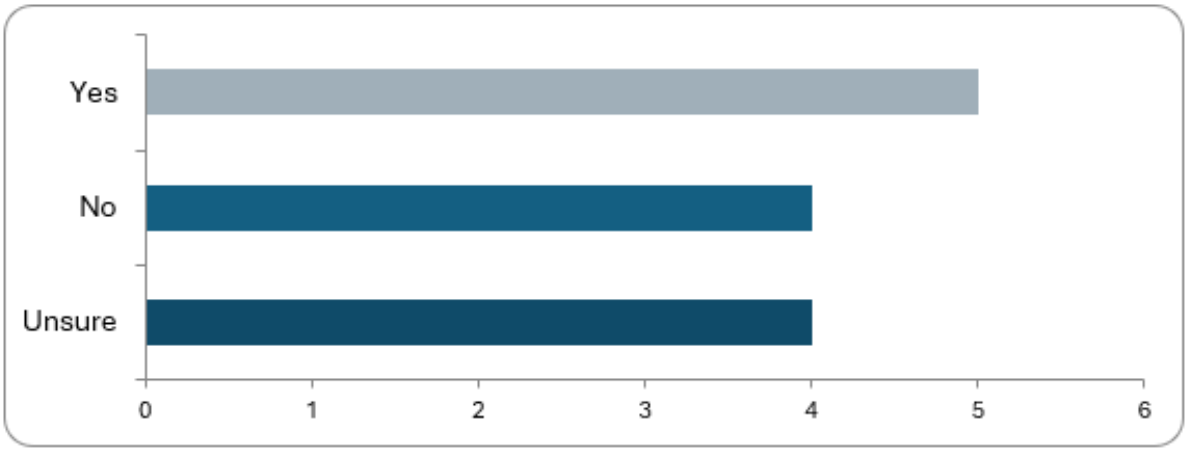
Option	Total	Percent
Yes	7	53.85%
No	1	7.69%
Unsure	5	38.46%
Not Answered	0	0.00%

Commentary

Generally, the view was that the reporting requirements were reasonable. One respondent felt that early notification could impact their customers but in doing so had failed to recognise that the reporting is confidential to the Technical Authority and onward communication, when necessary, would be sanitised to prevent the source being identified.

Q12: Are the thresholds for what constitutes a "significant impact" in Clause 31(3) clear?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	5	38.46%
No	4	30.77%
Unsure	4	30.77%
Not Answered	0	0.00%

Commentary

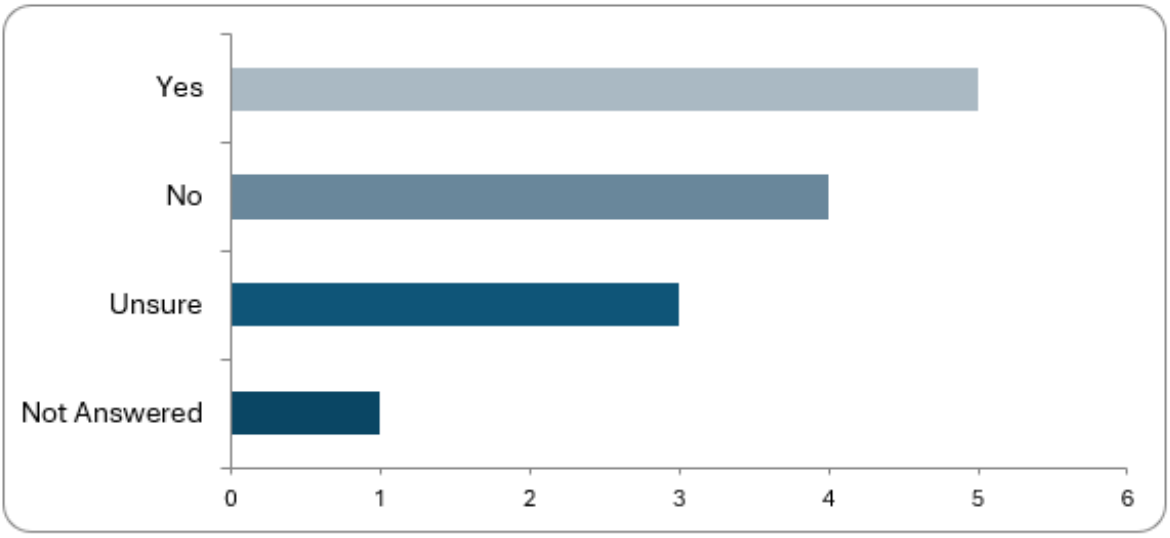
Generally, the responses were supportive with one respondent commenting:
"The multi-factor test allows contextual judgement and supports proportionate decision-making".

Some of the commentary regarding this question appeared to have been provided in isolation of other clauses which provide protections and interpretation. The criteria for identifying the significant impact is only used if the matter meets the requirements of a security incident in the first place and the requirements to report are based on an assessment by the registered provider who is best placed to make the assessment of risk or impact to the service.

Section 6: Compliance and Oversight

Q13: Are the powers of responsible authorities to assess compliance under Clauses 35–36 (including assessment notices and inspections) proportionate and clearly described?

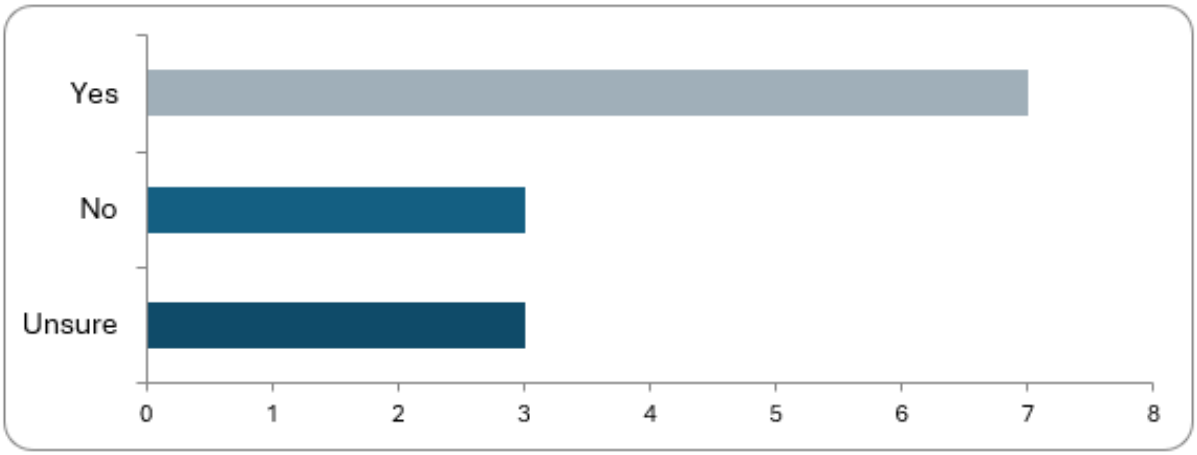
*There were **12** responses to this question.*



Option	Total	Percent
Yes	5	38.46%
No	4	30.77%
Unsure	3	23.08%
Not Answered	1	7.69%

Q14: Are the enforcement mechanisms in Clauses 39–43 effective and proportionate?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	7	53.85%
No	3	23.08%
Unsure	3	23.08%
Not Answered	0	0.00%

Commentary

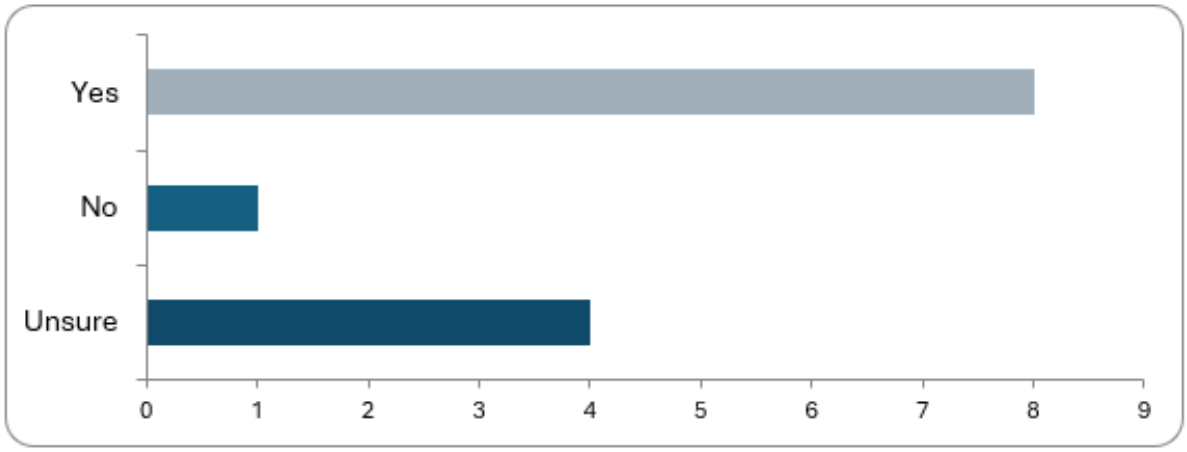
Several of the responses to questions 13 and 14 appear to have been drafted in isolation and had not recognised that these clauses only become applicable when certain non-compliances (i.e. security duties) are identified or suspected.

One respondent commented as follows:
"The powers are extensive but appropriately bounded by notice requirements, proportionality, and appeal rights."

Section 7: Designated Vendor Notices (DVNs), Designated Vendor Directions (DVDs) and Infrastructure Protection Orders (IPOs)

Q15: Are the criteria for issuing DVNs and DVDs under Clauses 47–49 and 57–59 clear and justified?

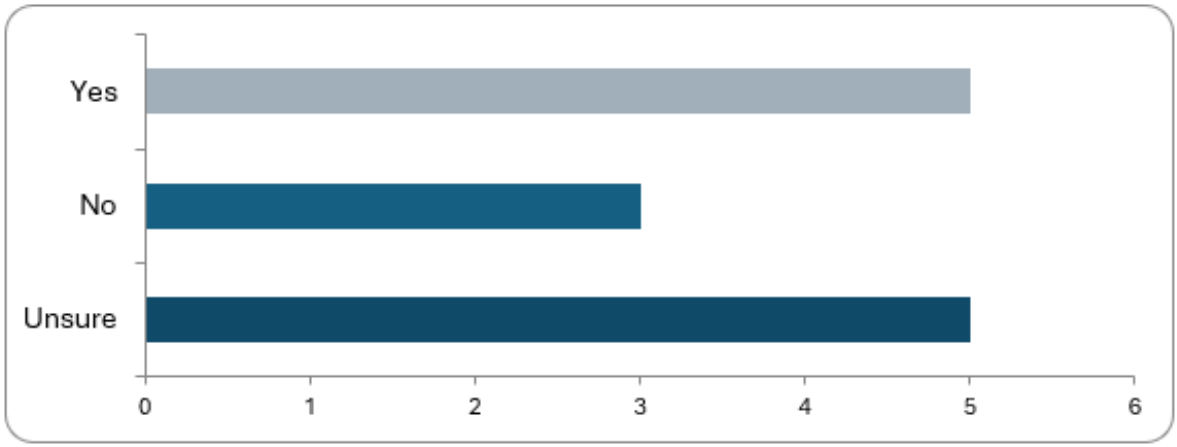
*There were **13** responses to this question.*



Option	Total	Percent
Yes	8	61.54%
No	1	7.69%
Unsure	4	30.77%
Not Answered	0	0.00%

Q16: Is the process for consultation, variation, and revocation of DVNs and DVDs (Clauses 47–49, 52–55 & 57) sufficiently transparent and accountable?

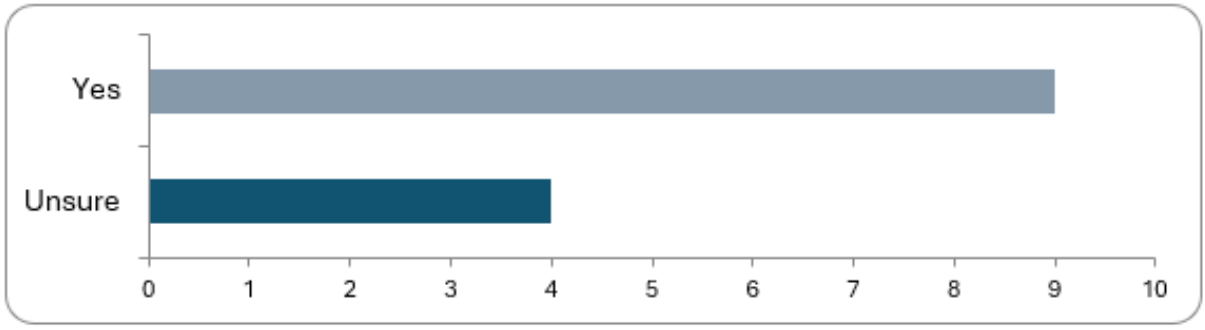
*There were **13** responses to this question.*



Option	Total	Percent
Yes	5	38.46%
No	3	23.08%
Unsure	5	38.46%
Not Answered	0	0.00%

Q17: Do Infrastructure Protection Orders (Clauses 68–71) provide a necessary complement to DVNs and DVDs?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	9	69.23%
No	0	0.00%
Unsure	4	30.77%
Not Answered	0	0.00%

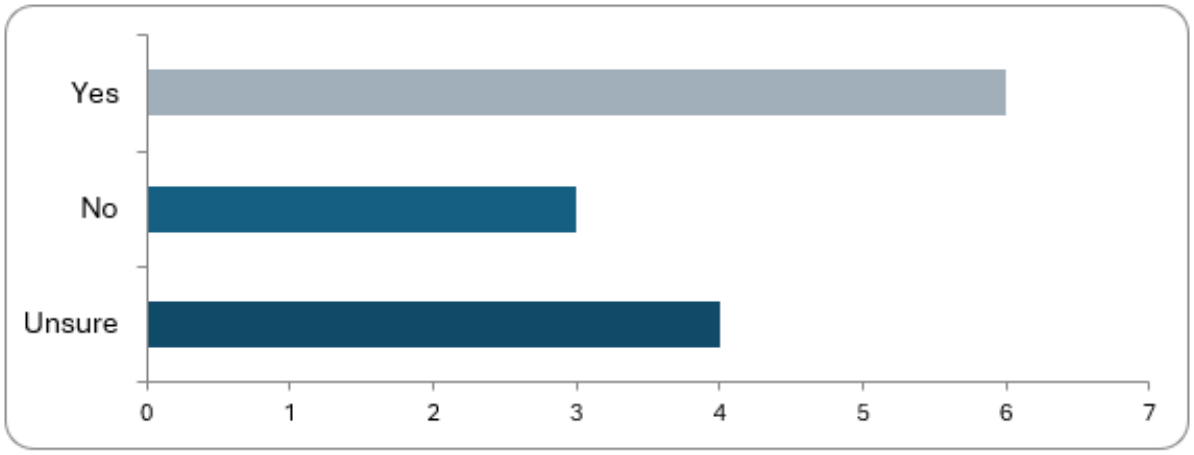
Commentary

Whilst the majority of respondents agreed that the criteria for issuing a Designated Vendor Notice and a Designated Vendor Direction were clear and that an Information Protection Order (IPO) provided a necessary complement to the Designated Vendor Notice (DVN) and Designated Vendor Direction (DVD), from some of the comments provided it was evident that some respondents may not have identified these orders (DVN,DVD and IPO's) are about national security risks.

DVN's and DVD's are only likely to be issued when there is deemed to be a serious threat to the CNI and the risk of that threat lies within the use of a certain Vendor services or equipment. An example in this scenario would be the suspected state interference into Huawei equipment that was deemed an unacceptable risk to the UK telecoms system of which the Isle of Man and the Channel Islands are users being part of the +44 International dialling code issued to the UK.

Q18: Are the criteria for issuing Infrastructure Protection Orders (IPOs) sufficiently clear and justified?

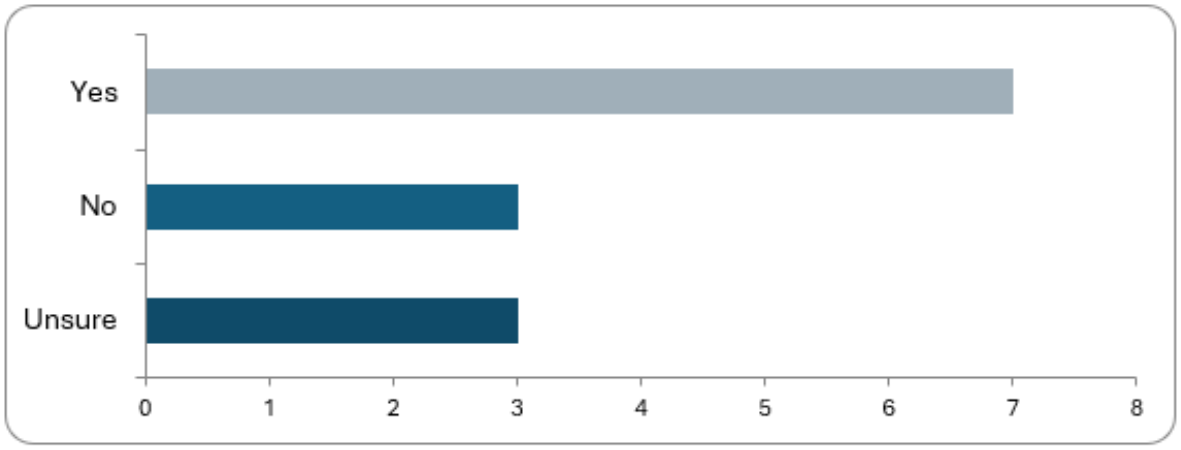
*There were **13** responses to this question.*



Option	Total	Percent
Yes	6	46.15%
No	3	23.08%
Unsure	4	30.77%
Not Answered	0	0.00%

Q19: Should IPOs be subject to additional safeguards or oversight mechanisms?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	7	53.85%
No	3	23.08%
Unsure	3	23.08%
Not Answered	0	0.00%

Commentary

Generally, respondents were supportive of Infrastructure Protection Orders (IPO's) and a review of the comments provided identified the conditions that are required to be met before an IPO can be issued may have been overlooked.

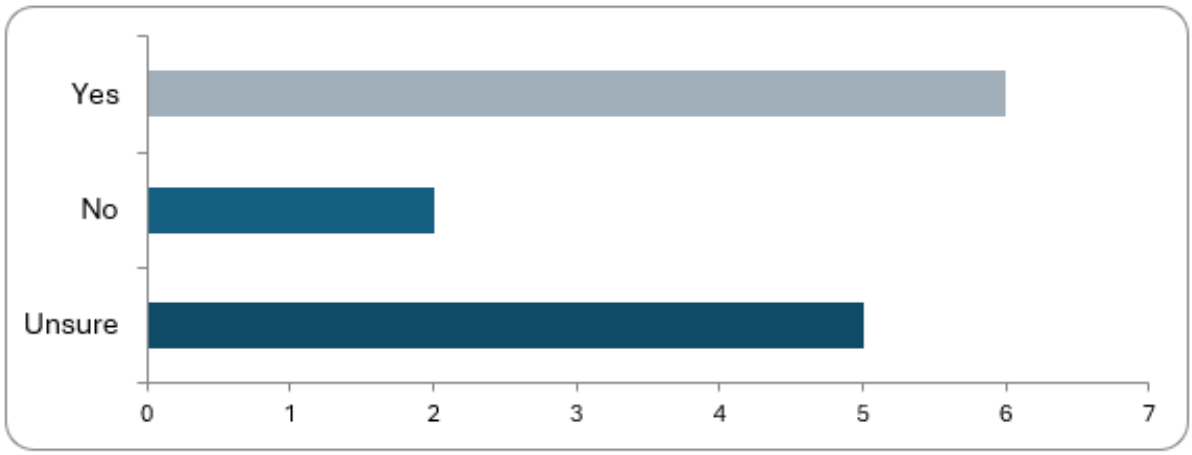
In order for an IPO to be issued the following would need to occur:

- *The Department is aware of a serious risk or unacceptable threat to an ESSENTIAL service, and*
- *is unable to find another avenue to mitigate the matter.*
- *An IPO can only exist for 3 months and is to protect that service during the time whilst mitigation or solution is sought.*

Section 8: Information Requests and Non-Disclosure

Q20: Are the powers to request information under Clauses 72–74 proportionate and clearly limited by safeguards in Clause 73?

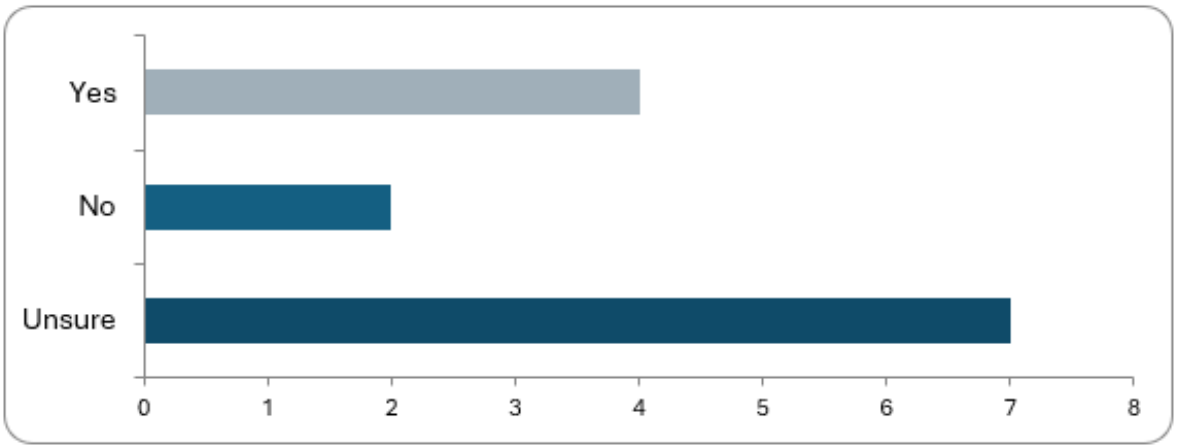
*There were **13** responses to this question.*



Option	Total	Percent
Yes	6	46.15%
No	2	15.38%
Unsure	5	38.46%
Not Answered	0	0.00%

Q21: Are the non-disclosure provisions in Clause 67 (including restrictions on sharing the contents of certain notices or directions) clear, proportionate, and necessary for national security?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	4	30.77%
No	2	15.38%
Unsure	7	53.85%
Not Answered	0	0.00%

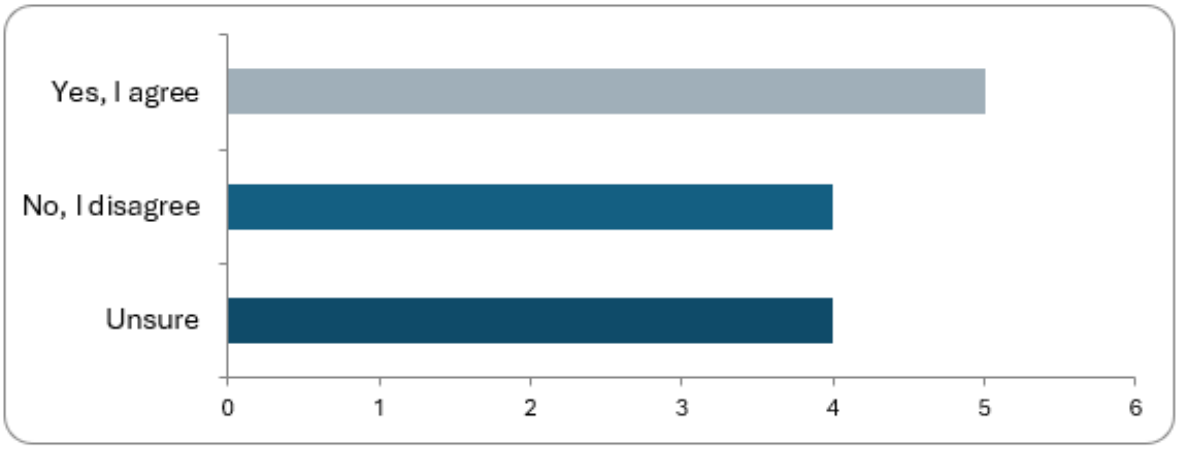
Commentary

The responses provided were generally positive and where an unsure response was submitted the comments indicated that it had not been recognised that these restrictions only relate to when a Designated Vendor Notice (DVN), Designated Vendor Direction (DVD) or Infrastructure Protection Order (IPO) had been issued. Where there was a requirement not to disclose the contents of a DVN, DVD or IPO clause 67(10) states that this would only be where the Department considers that disclosure would be contrary to national security.

Section 9: Fines and Penalties

Q22: Do you agree that the proposed fines and penalties are proportionate to the risks posed by non-compliance?

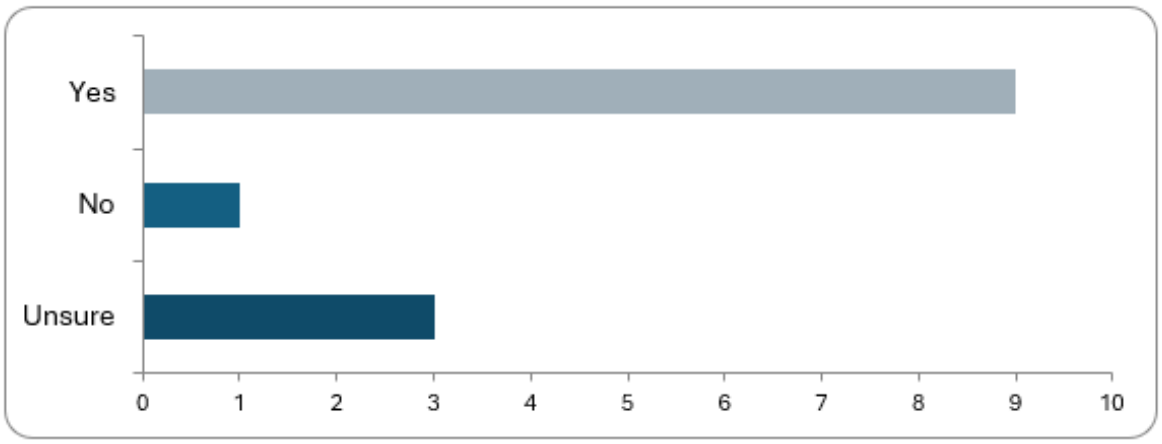
*There were **13** responses to this question.*



Option	Total	Percent
Yes	5	38.46%
No	4	30.77%
Unsure	4	30.77%
Not Answered	0	0.00%

Q23: Is the distinction between civil penalties and enforcement actions (e.g. urgent directions, tribunal appeals) clear and appropriate?

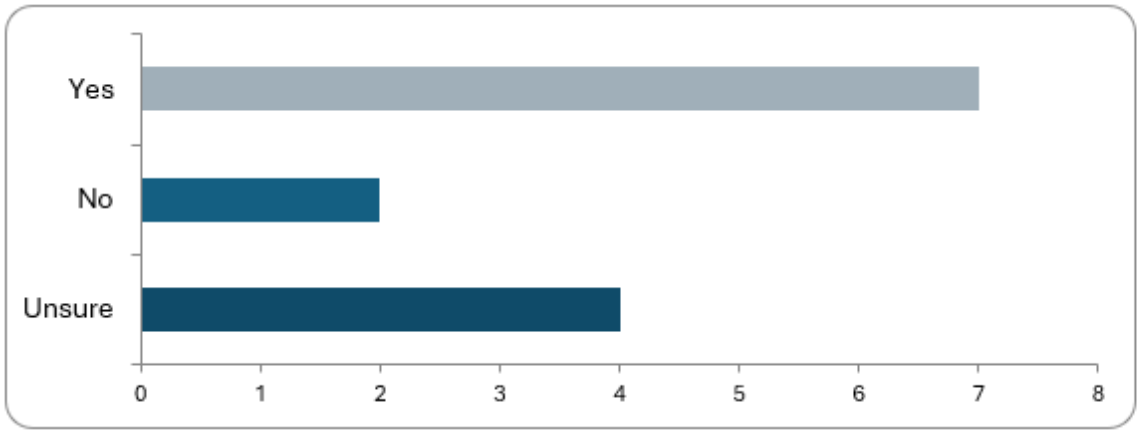
*There were **13** responses to this question.*



Option	Total	Percent
Yes	9	69.23%
No	1	7.69%
Unsure	3	23.08%
Not Answered	0	0.00%

Q24: Do you support the use of higher penalties for breaches involving designated vendors or national security risks?

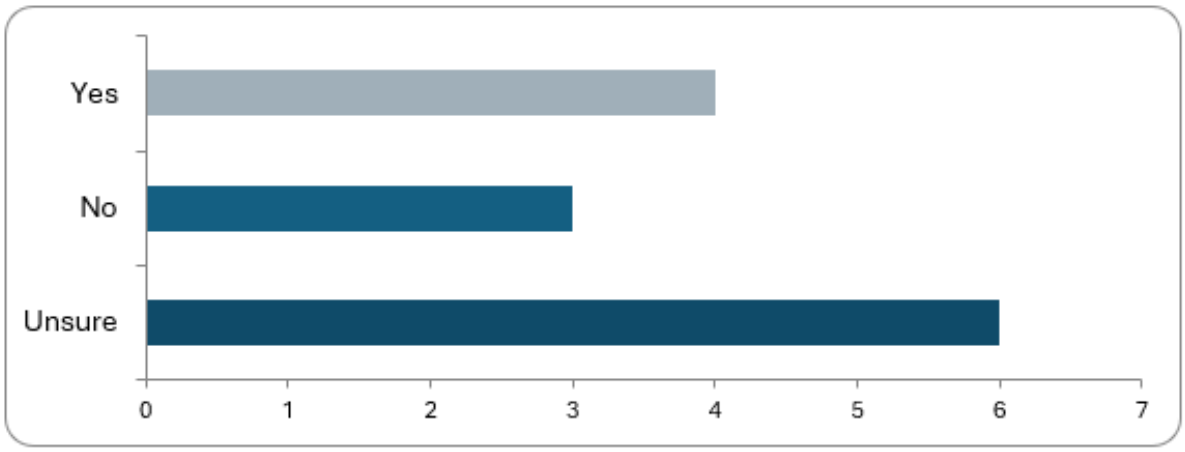
*There were **13** responses to this question.*



Option	Total	Percent
Yes	7	53.85%
No	2	15.38%
Unsure	4	30.77%
Not Answered	0	0.00%

Q25: Does the Bill strike the right balance between encouraging compliance and enabling enforcement?

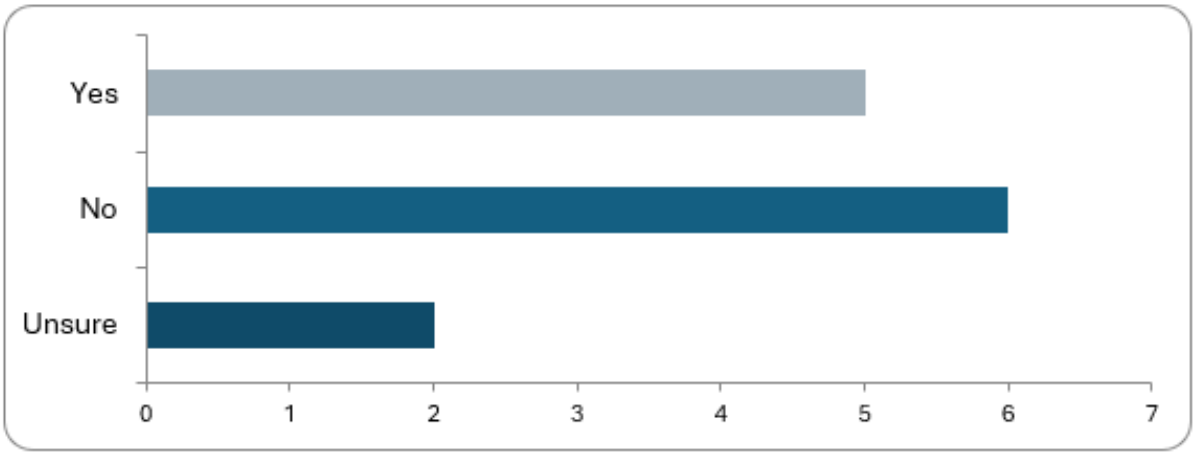
*There were **13** responses to this question.*



Option	Total	Percent
Yes	4	30.77%
No	3	23.08%
Unsure	6	46.15%
Not Answered	0	0.00%

Q26: Are there any additional safeguards or considerations you believe should be included in the enforcement framework?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	5	38.46%
No	6	46.15%
Unsure	2	15.38%
Not Answered	0	0.00%

Commentary

In the main, the responses to these questions were positive.

One respondent commented:
"The linkage to severity and turnover is appropriate for deterrence, provided penalties are applied proportionately."

Several comments referred to the level of penalties that may be imposed.

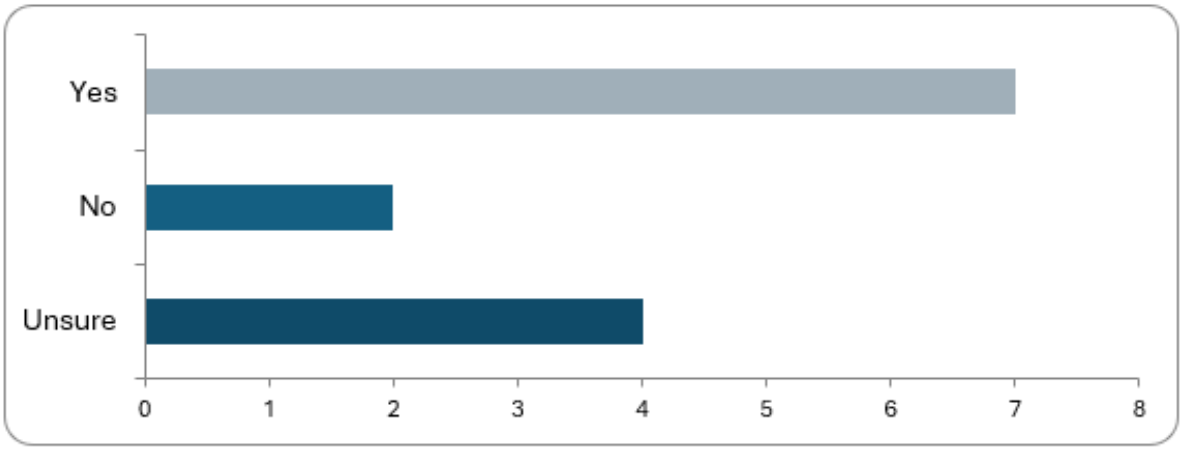
However, these comments also suggest that it may not have been appreciated that these are maximum penalties.

In addition, Clause 80 includes a proportionality test at 80(3) which requires the Responsible Authority to consider four criteria when establishing a penalty and that Clause 80(10) affords a right of appeal to a tribunal.

Section 10: Codes of Practice and Assurance Frameworks

Q27: Is the role of codes of practice and assurance frameworks (Clauses 23, 75–79) in supporting compliance clearly articulated?

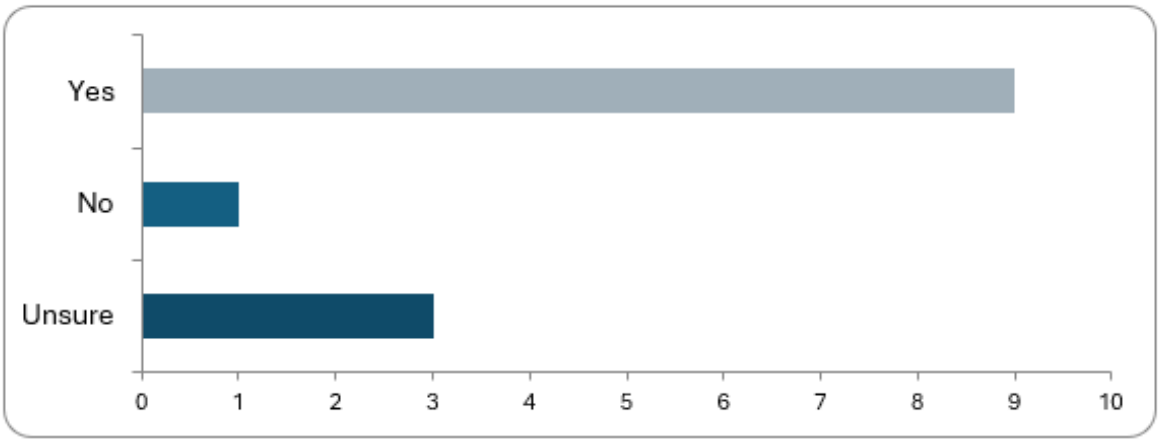
*There were **13** responses to this question.*



Option	Total	Percent
Yes	7	53.85%
No	2	15.38%
Unsure	4	30.77%
Not Answered	0	0.00%

Q28: Are the procedures for issuing, revising, and withdrawing codes of practice (Clauses 75–77) sufficiently robust?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	9	69.23%
No	1	7.69%
Unsure	3	23.08%
Not Answered	0	0.00%

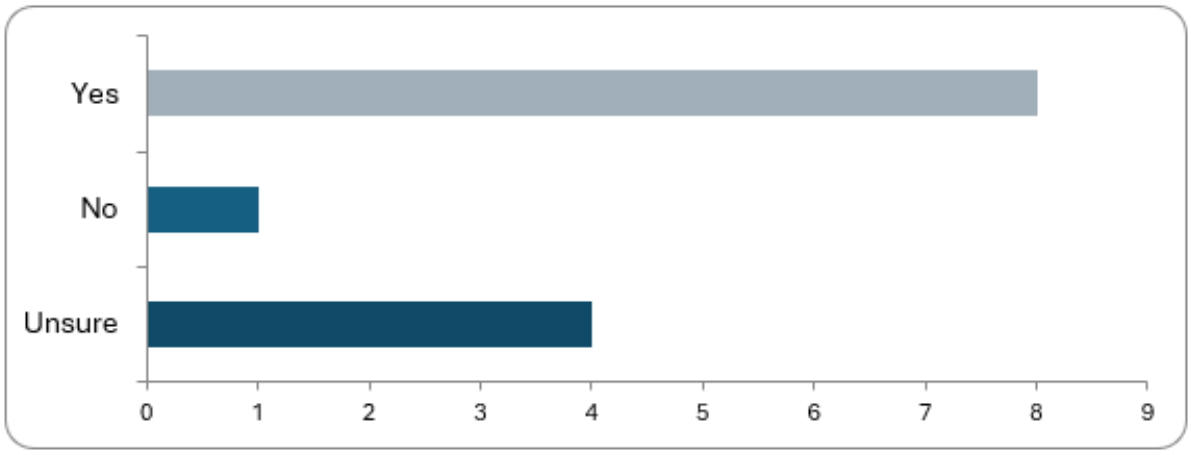
Commentary

Generally, there was support for the processes surrounding Codes of Practice.

Section 11: Reporting and Monitoring

Q29: Are the reporting obligations for Responsible Authorities and the Technical Authority in Clauses 13 and 20 clearly defined and appropriate?

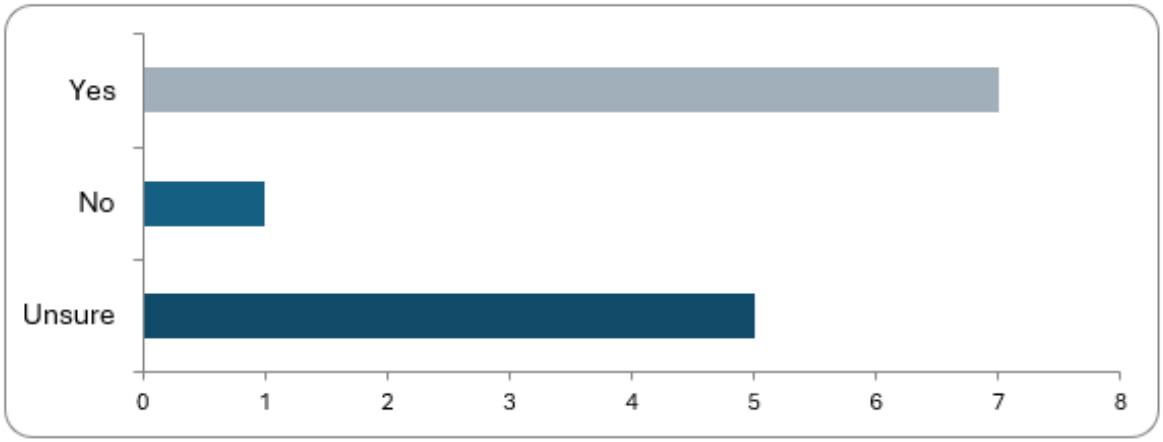
*There were **13** responses to this question.*



Option	Total	Percent
Yes	8	61.54%
No	1	7.69%
Unsure	4	30.77%
Not Answered	0	0.00%

Q30: Are the frequency and content of required reports for entities (e.g. annual reports, security reports) suitable for effective oversight?

*There were **13** responses to this question.*



Option	Total	Percent
Yes	7	53.85%
No	1	7.69%
Unsure	5	38.46%
Not Answered	0	0.00%

Commentary

Respondents were generally supportive of the approach to reporting obligations to the Responsible and Technical Authorities.

Where respondents were unsure, this reflected the fact that as this was only proposed legislation, there was no practical experience to base their response on.

Section 12: Implementation

Q31: What support or guidance would your organisation need to comply with the proposed legislation?

*There were **10** responses to this question.*

Q32: What role should government play in helping smaller or less-resourced entities meet their obligations?

*There were **10** responses to this question.*

Commentary

The Responsible Authorities and the Technical Authority were requested to produce guidance to support the introduction and ongoing implementation of the Bill.

Ongoing consultation and engagement was also requested as was reflected in the following comments:
"We support the intended outcome of this important legislation. We most value active and constructive consultation on various items, as raised, to ensure that the intended outcomes are achieved in the most efficient manner."

"Clear, practical guidance distinguishing technical cyber-security obligations from non-technical issues would be essential, particularly for smaller entities."

"A breakdown of the bill through a practical handbook or checklist which would make the new requirements easily understood would significantly help businesses comply with the proposed legislation. This should be complemented by clear guidance on the standards and frameworks that would become applicable as a result of the legislation."

The Department has already published a guide to the proposed Bill and will continue to produce further advice and guidance to support the introduction of the Bill.